Akıllı Çocuk Saatleri

written by Mert SARICA | 1 September 2022
If you are looking for an English version of this article, please visit here.

Bu hikaye, 4 Mayıs 2022 tarihinde Erman ATEŞ isimli bir okurumdan aldığım e-posta ile başladı. Bilinçli ve duyarlı bir baba olan Erman Bey göndermiş olduğu e-postada, akıllı çocuk saatlerinin bir çok ebeveyn tarafından haklı gerekçelerle tercih edilmeye başlandığını ancak yazılım, güvenlik ve mahremiyet açısından hem bir standarda tabi olmamaları hem de Instagram'da gördüğü bir mesaj nedeniyle tüm ebeveynler adına endişe duymaya başladığını ve bu nedenle de bu konuya mercek tutmamı rica etmişti. Instagram Dolandırıcıları, Arka Kapı Avı, Tuzak Sistem ile Hacker Avı blog yazılarımda olduğu gibi okurlarına her daim kulak veren bir güvenlik araştırmacısı olarak toplumsal fayda ve bilgi güvenliği farkındalığı adına bu konuya eğilmeye karar verdim.

Konu:
çocuklar için akıllı saatler

Mesajınız:
Merhaba Mert Bey,

Sizleri yıllardır ilgiyle takip ediyorum.

Ben 9 yaşında bir erkek çocuk babasıyım ve çocukların takip edilebildiği akıllı dijital saatlerin bir çok anne baba tarafından tercih edilmeye başlandığını görmekteyim. Nitekim cihazlar ve içlerindeki yazılımlar standardlara uyan ve lisans sahibi değiller genellikle.

Bazı instagram hesaplarında sadece belirli numaralardan aranması gerekirken herhangi birinin arayabildiği, sim kartın internet erişimi sağlaması vesilesiyle saate bağlanılarak ses ve video kaydı alınabilmesi gibi çeşitli endişelerin baş gösterdiğini görüyorum.

dijitalbaba orhan toker beyin instagram hesabı ve web sayfalarında bu konuyla ilgili birkaç paylaşım gördüm ve hem kendi ailem hem de birçok aile için endişelenmeye başladım.

bu konuda farkındalığı artırmak amacıyla sizlerin akıllı saatlerin güvenliği konusunda bir araştırma/değerlendirme bloğu yazmanızın mümknü olup olamayacağını sormak isterim (inanıyorum bu konuda size yazan ilk kişi ben değilimdir).

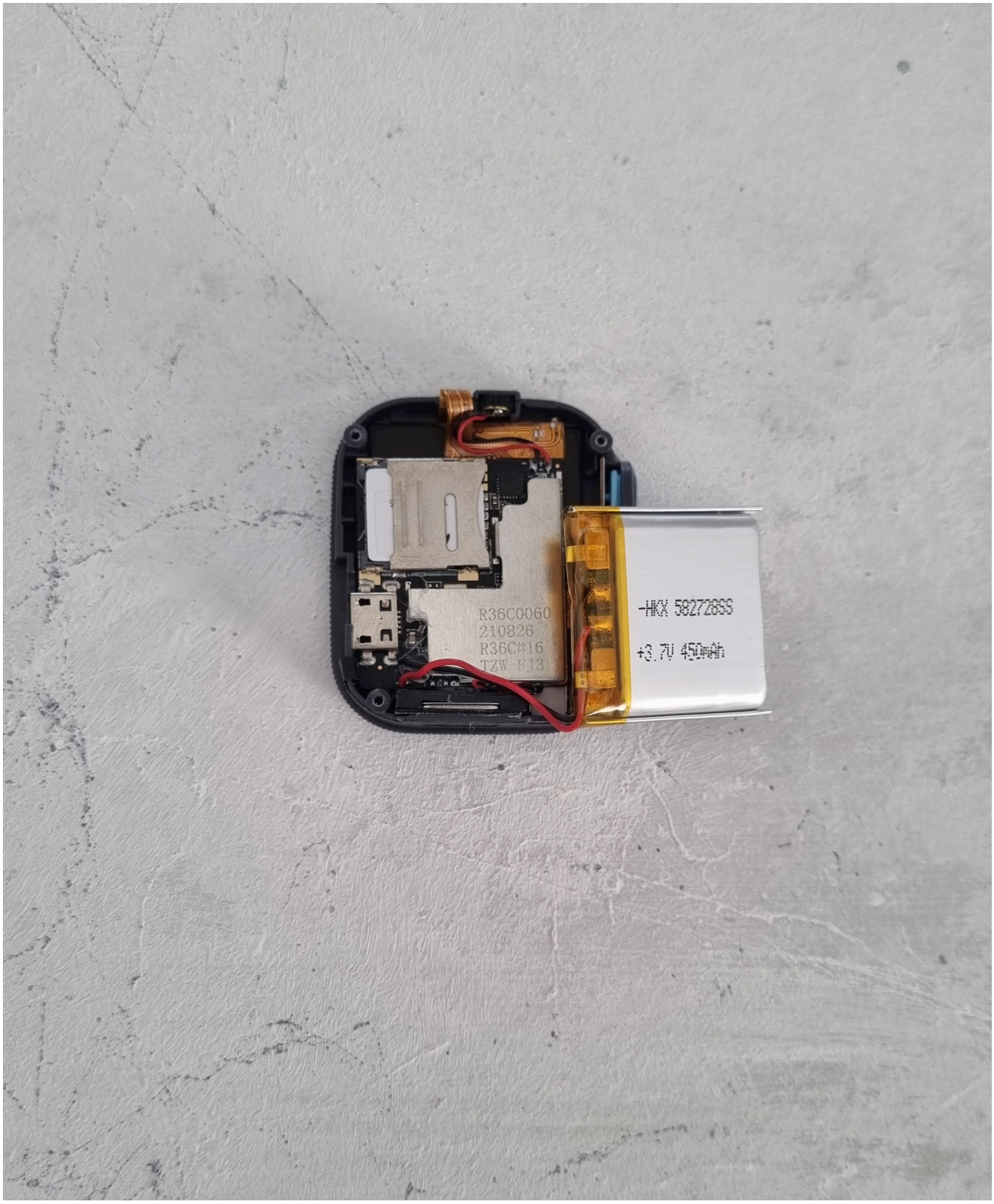
Teşekkürler, saygılar.

Erman

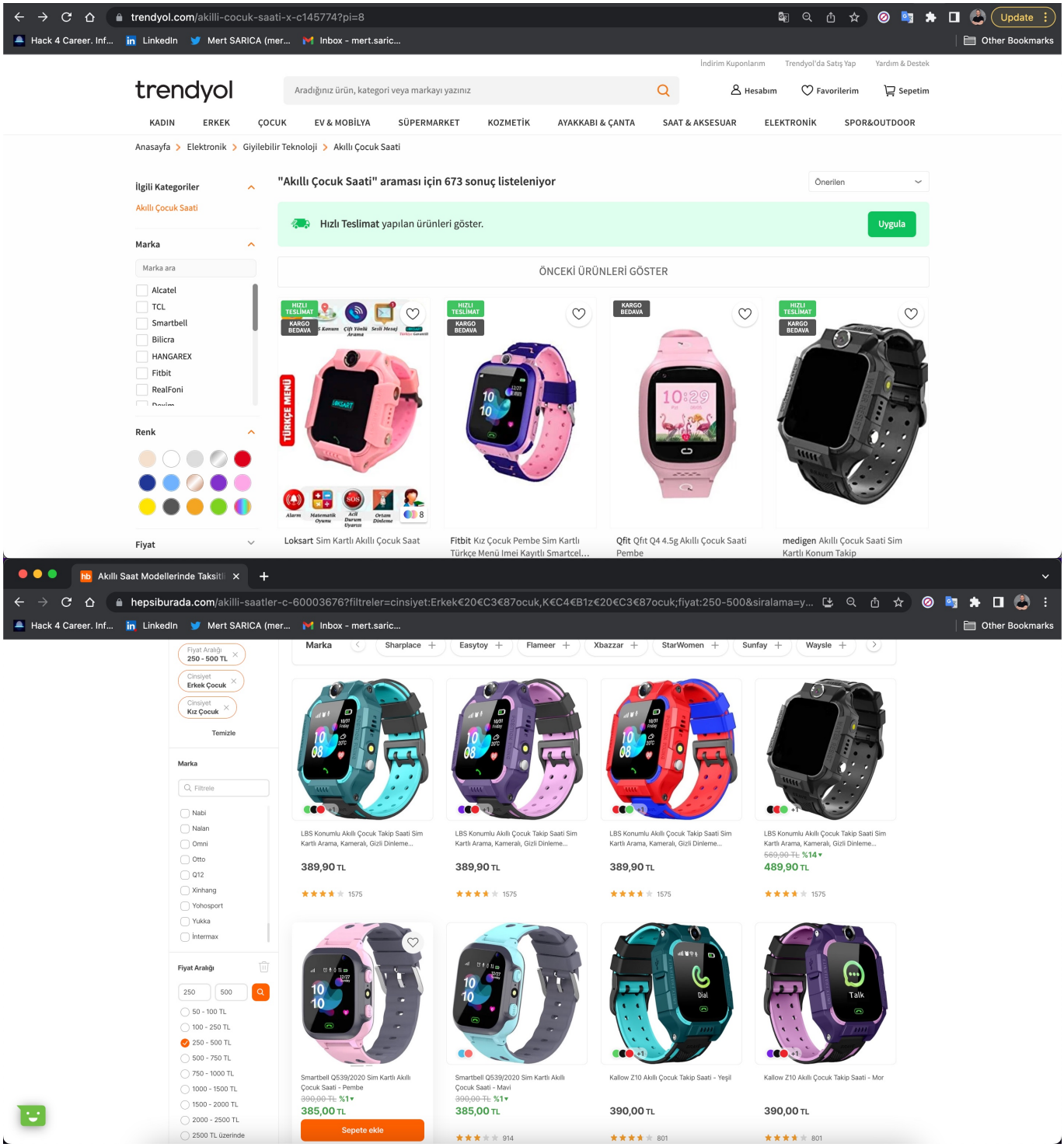
Aşağıdaki fotoğrafa bakıldığında akıllı çocuk saatleri gerçekten ebeveynler için çocuklarını gözetim altında tutmak için faydalanabilecekleri büyük bir teknolojik nimet mi ?



Yoksa aşağıdaki diğer bir fotoğrafa bakıldığında ebeveynlerin, kendilerinin ve çocuklarının mahremiyetini, özel hayatlarının gizliliğini istemeden de olsa tehlikeye attıkları, ortam dinlemeye imkan tanıyan saat görünümlü potansiyel casus bir cihaz mı ?



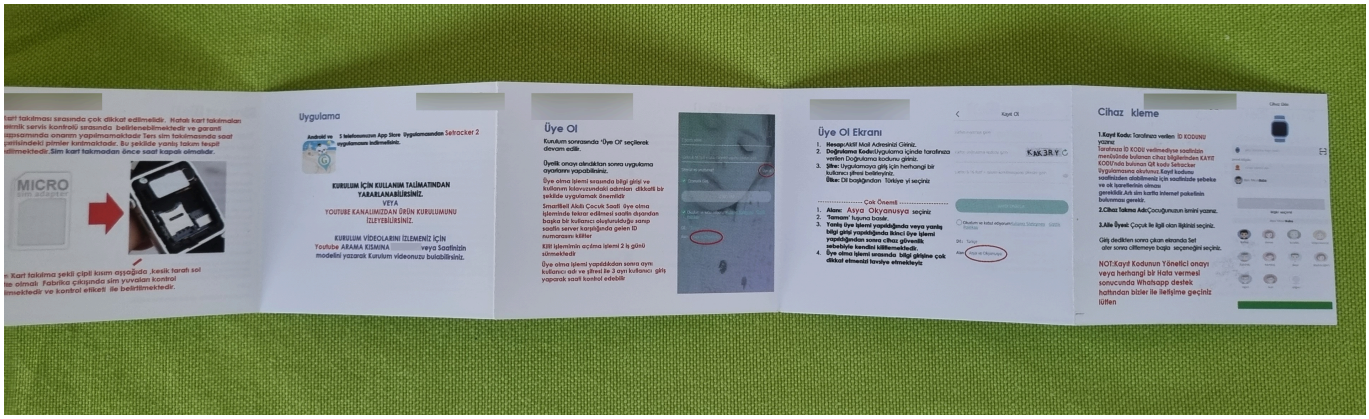
Bu sorulara yanıt bulmak için ilk olarak güvenlik araştırmamda kullanmak üzere fiyat açısından uygun olan bir çocuk saati satın almaya karar verdim. Bunun için Hepsiburada, Trendyol gibi alışveriş sitelerindeki Akıllı Çocuk Saatleri kategorilerini incelemeye başladım. En çok satılan, yorum ve değerlendirme yapılan saatlere baktıktan sonra 1000‘e yakın değerlendirmesi olan bir marka ve modelde karar kılıp, satın aldım.


trendyol.com/akilli-cocuk-saati-x-c145774?pi=8
Update
Hack 4 Career. Inf...
LinkedIn
Mert SARICA (mer...
Inbox - mert.saric...
Other Bookmarks
İndirim Kuponlarım
Trendyol'da Satış Yap
Yardım & Destek
trendyol
Aradığınız ürün, kategori veya markayı yazınız
Hesabım
Favorilerim
Sepetim
KADIN
ERKEK
ÇOCUK
EV & MOBİLYA
SÜPERMARKET
KOZMETİK
AYAKKABI & ÇANTA
SAAT & AKSESUAR
ELEKTRONİK
SPOR&OUTDOOR
Anasayfa
Elektronik
Giyilebilir Teknoloji
Akıllı Çocuk Saati
İlgili Kategoriler
Akıllı Çocuk Saati
Marka
Marka ara
Alcatel
TCL
Smartbell
Bilicra
HANGAREX
Fitbit
RealFoni
Renk
Fiyat
"Akıllı Çocuk Saati" araması için 673 sonuç listeleniyor
Önerilen
Hızlı Teslimat yapılan ürünleri göster.
Uygula
ÖNCEKİ ÜRÜNLERİ GÖSTER
HIZLI TESLİMAT
KARGO BEDAVA
TÜRKÇE MENÜ
Loksart Sim Kartlı Akıllı Çocuk Saat
Fitbit Kız Çocuk Pembe Sim Kartlı Türkçe Menü İmei Kayıtlı Smartcel...
Qfit Qfit Q4 4.5g Akıllı Çocuk Saati Pembe
medigen Akıllı Çocuk Saati Sim Kartlı Konum Takip
Akıllı Saat Modellerinde Taksitli
hepsiburada.com/akilli-saatler-c-60003676?filtreler=cinsiyet:Erkek€20€C3€87ocuk,K€C4€B1z€20€C3€87ocuk;fiyat:250-500&siralama=y...
Fiyat Aralığı 250 - 500 TL
Cinsiyet Erkek Çocuk
Cinsiyet Kız Çocuk
Temizle
Marka
Filtrele
Nabi
Nalan
Omni
Otto
Q12
Xinhang
Yohosport
Yukka
İntermax
Fiyat Aralığı
50 - 100 TL
100 - 250 TL
250 - 500 TL
500 - 750 TL
750 - 1000 TL
1000 - 1500 TL
1500 - 2000 TL
2000 - 2500 TL
2500 TL üzerinde
Sharplace
Easytoy
Flameer
Xbazzar
StarWomen
Sunfay
Waysle
LBS Konumlu Akıllı Çocuk Takip Saati Sim Kartlı Arama, Kameralı, Gizli Dinleme...
389,90 TL
1575
489,90 TL
%14
Smartbell Q539/2020 Sim Kartlı Akıllı Çocuk Saati - Pembe
385,00 TL
Sepete ekle
Smartbell Q539/2020 Sim Kartlı Akıllı Çocuk Saati - Mavi
Kallow Z10 Akıllı Çocuk Takip Saati - Yeşil
390,00 TL
Kallow Z10 Akıllı Çocuk Takip Saati - Mor
914
801


KONTROL EDİLMİŞTİR
ÜRÜNÜ 2 SAAT BOYUNCA POWER BANK VEYA BİLGİSAYAR İLE ŞARJ EDİNİZ.
AKSİ TAKDİRDE ÜRÜN GARANTİ KAPSAMI DIŞINDA KALACAKTIR.

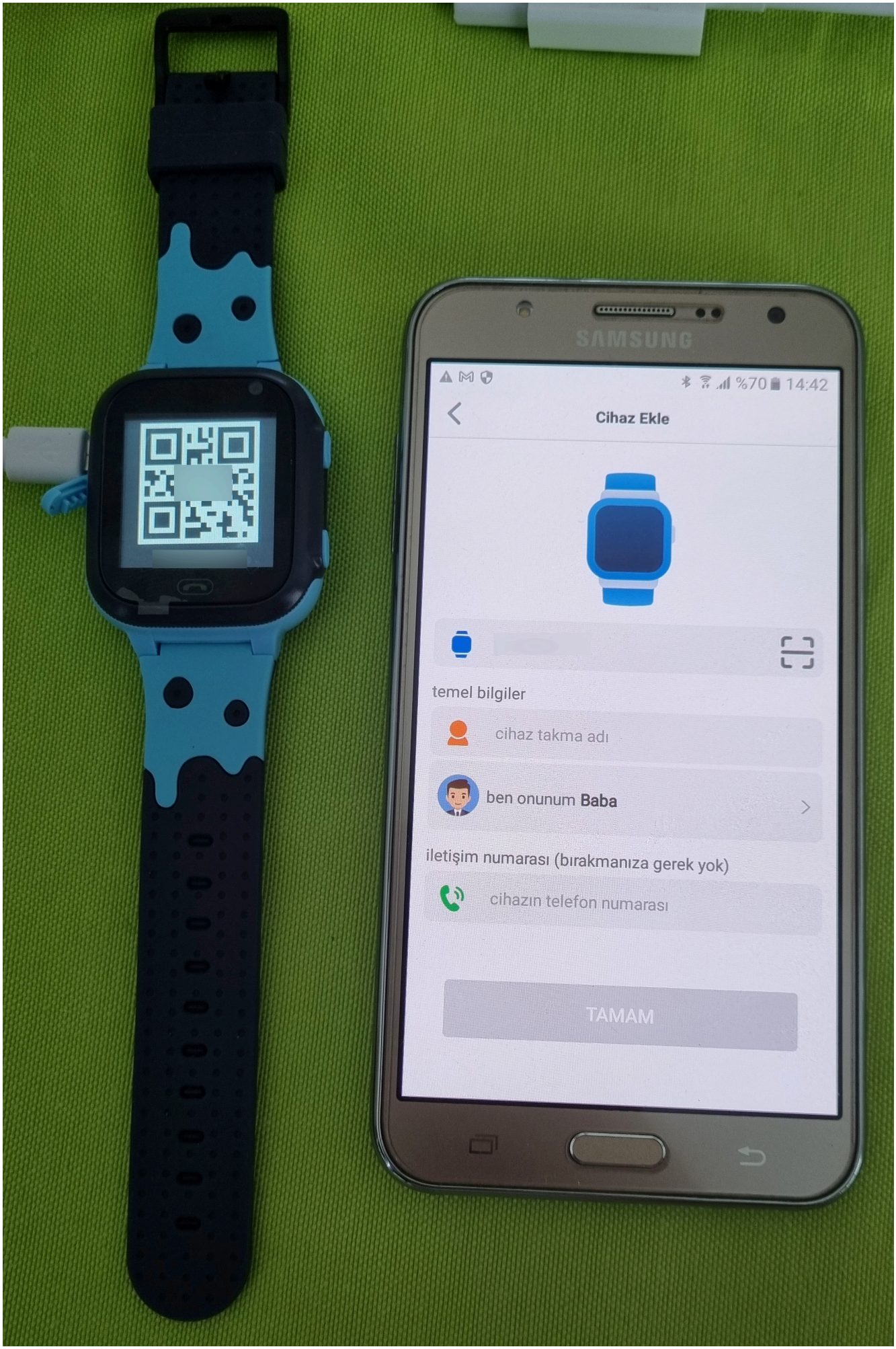


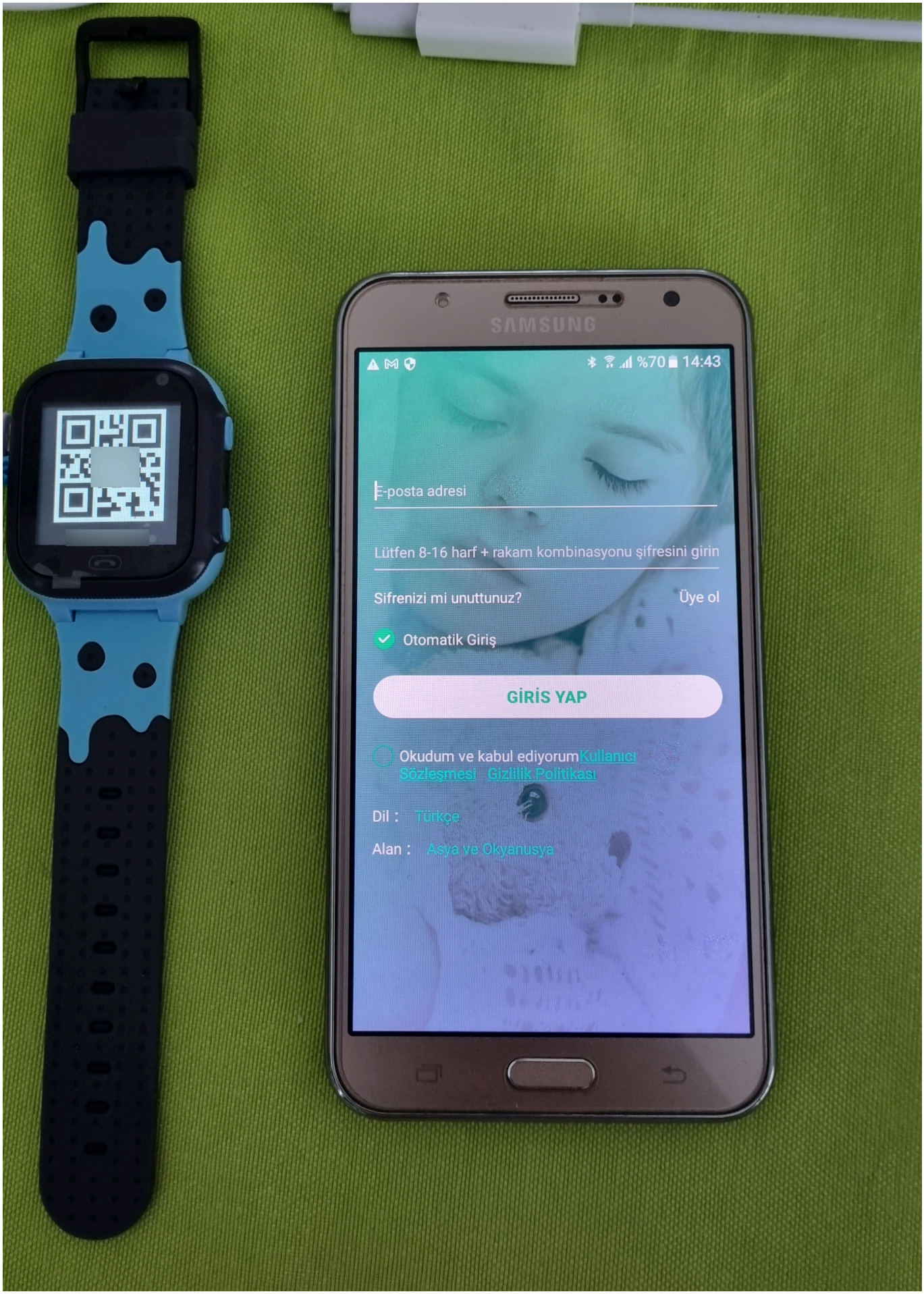
Saati kutusundan çıkarıp, kurulum kılavuzunu incelediğimde, saati uzaktan yönetebilmek için Çinli 3G Electronics isimli bir şirket tarafından geliştirilen Android veya iOS mobil uygulamasının kurulmasının gerektiği belirtiliyordu.

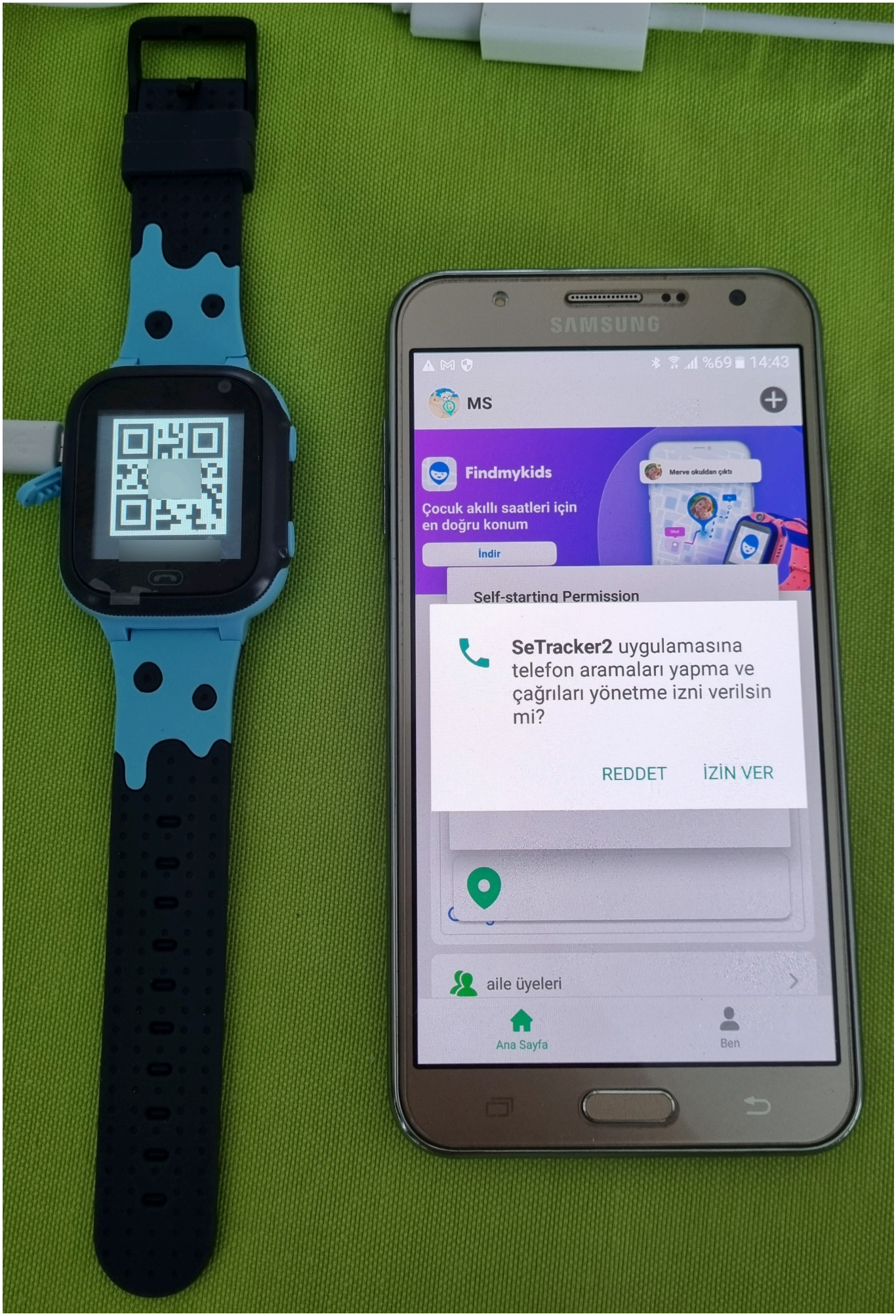


SeTracker2 isimli uygulamanın topladığı bilgilere baktığımızda lokasyon, ses ve görüntü kaydından, rehbere, isim, cep telefonu ve e-posta adresine kadar kişiye özel, hassas, mahrem sayılabilecek bilgiler olduğunu gördüm.

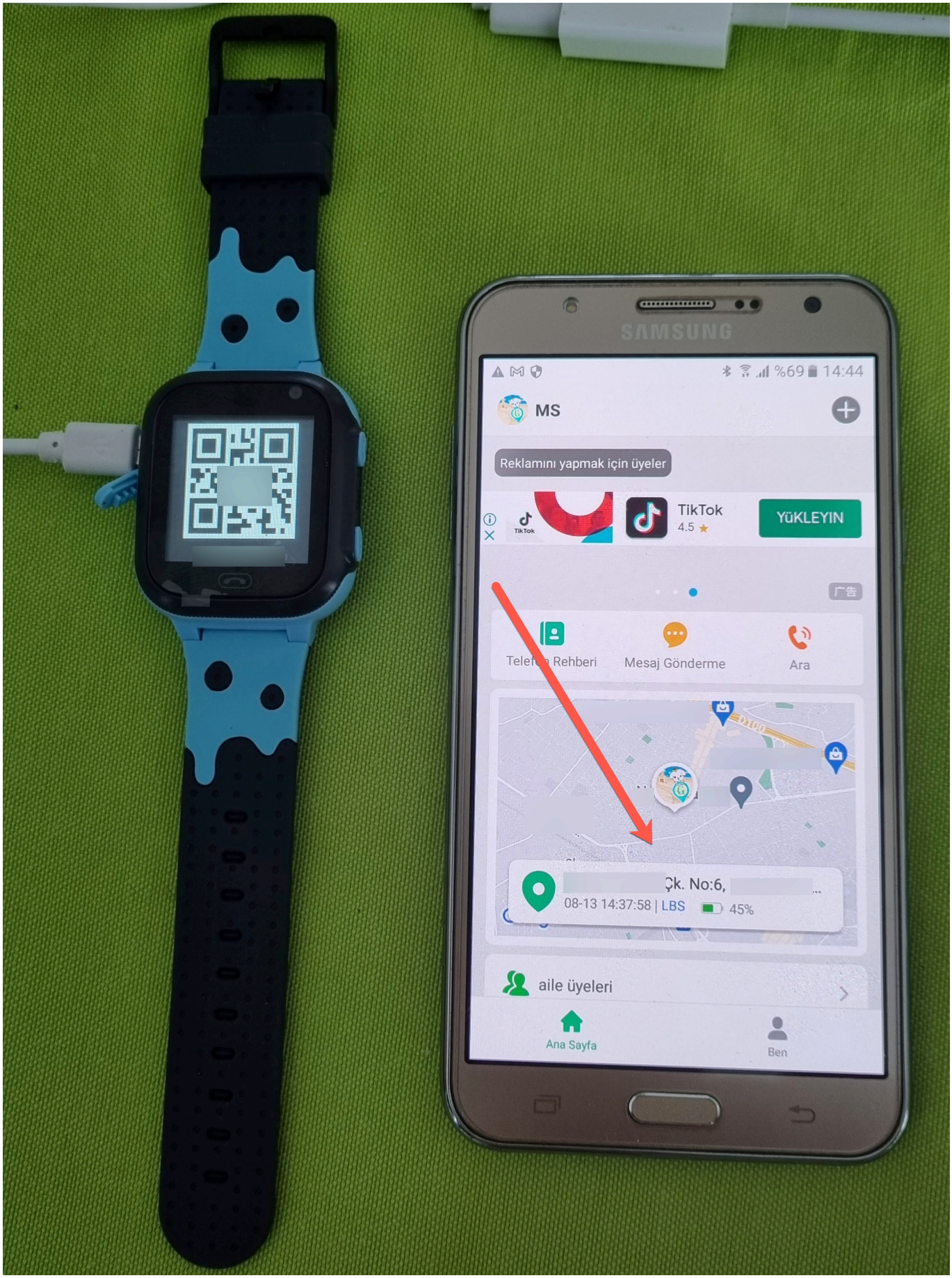
Saate SIM kartı takıp, çalıştırdıktan sonra SeTracker2 uygulamasını açıp, kayıt oldum. Daha sonra uygulamaya ile saati eşleştirdikten sonra uygulamayı ve menü adımlarını incelemeye başladım.

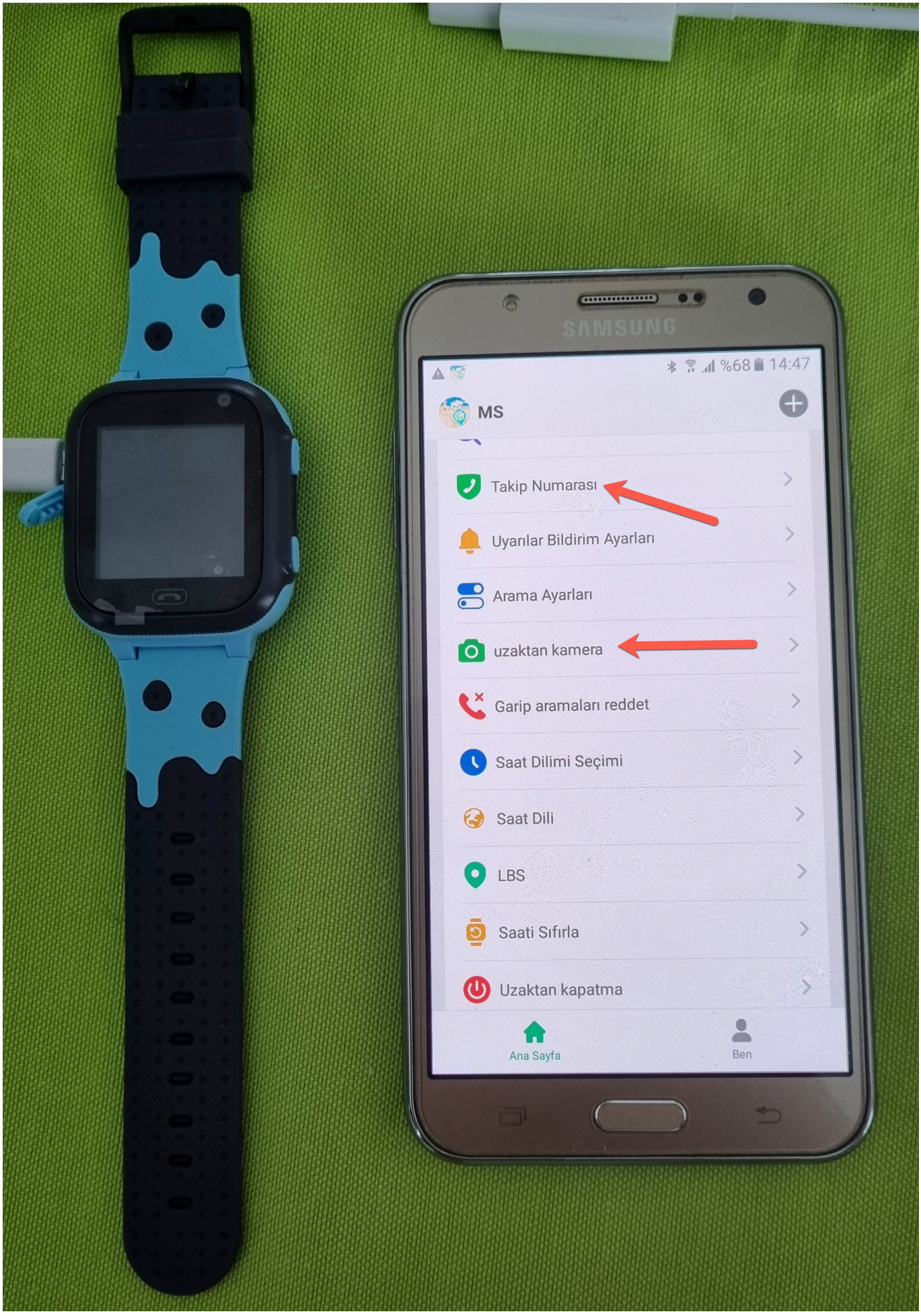

SAMSUNG
%70 14:42
Cihaz Ekle
temel bilgiler
cihaz takma adı
ben onunum Baba
iletişim numarası (bırakmanıza gerek yok)
cihazın telefon numarası
TAMAM

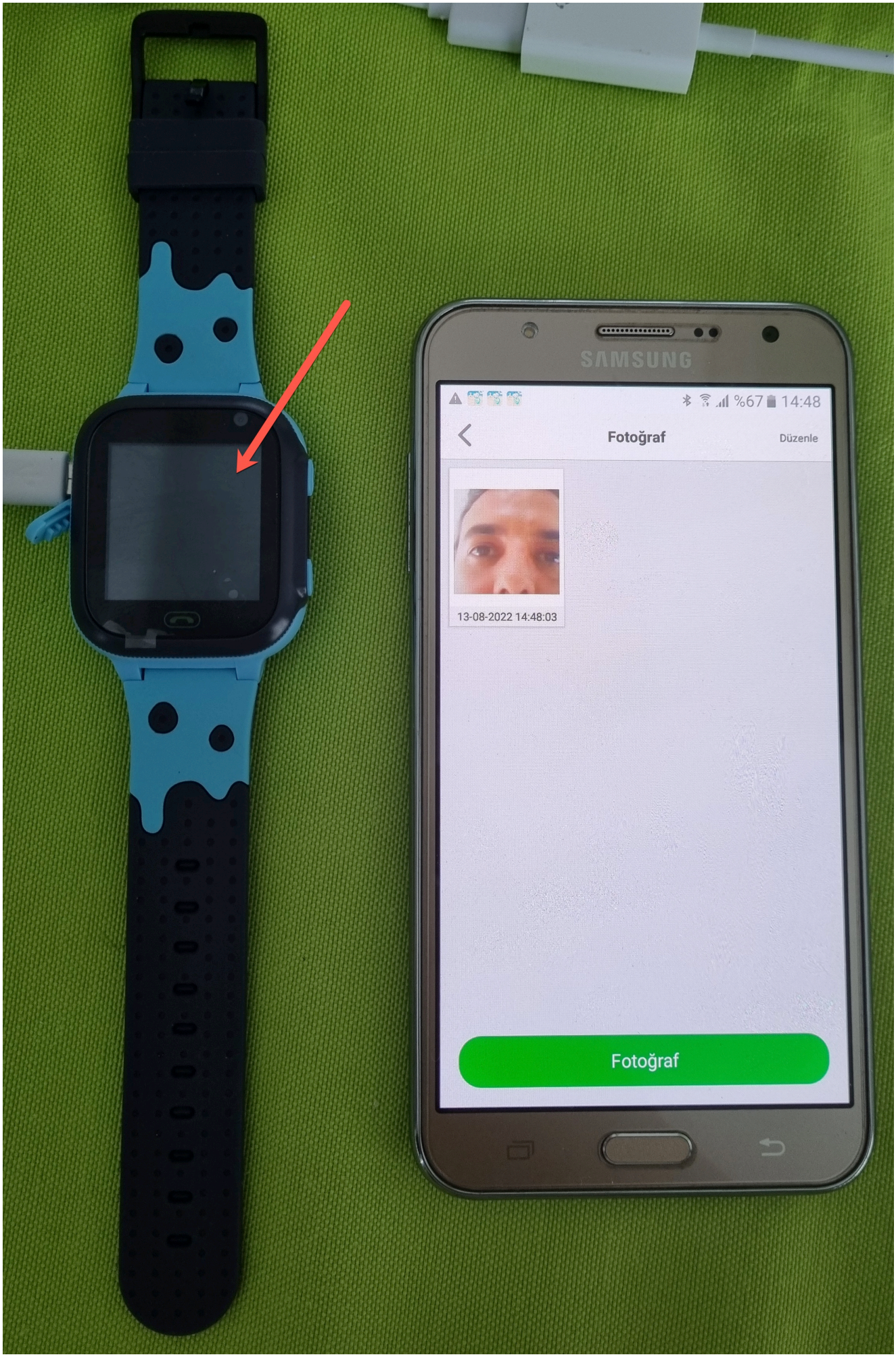

SAMSUNG
%70 14:43
E-posta adresi
Lütfen 8-16 harf + rakam kombinasyonu şifresini girin
Sifrenizi mi unuttunuz?
Üye ol
Otomatik Giriş
GİRİS YAP
Okudum ve kabul ediyorum Kullanıcı Sözleşmesi Gizlilik Politikası
Dil : Türkçe
Alan : Asya ve Okyanusya


SAMSUNG
%69 14:43
MS
Findmykids
Çocuk akıllı saatleri için
en doğru konum
İndir
Merve okuldan çıktı
Self-starting Permission
SeTracker2 uygulamasına telefon aramaları yapma ve çağrıları yönetme izni verilsin mi?
REDDET
İZİN VER
aile üyeleri
Ana Sayfa
Ben

Uygulamada öncelikle dikkatimi çeken nokta, saatin harita üzerinden anlık olarak izlenebilmesi daha sonra ise Takip Numarası ve uzaktan kamera menü adımları oldu. Uzaktan kamera menüsü üzerinden saatteki kamera ile istediğiniz zaman fotoğraf çekilebiliyorsunuz. Bu esnada saat herhangi bir görsel veya işitsel bir uyarı oluşturmuyor. Takip numarası menüsü ile ise saatin girilen cep telefonu numarasını aramasını sağlayabiliyorsunuz ve saatteki mikrofon sayesinde de ortam dinlemesi yapılabiliyor. Bu esnada yine uzaktan kamera adımında olduğu gibi telefon, ortam dinlemesi yapıldığına dair herhangi bir uyarı vermiyor.


SAMSUNG
%69 14:44
MS
Reklamını yapmak için üyeler
TikTok
4.5
YÜKLEYIN
Mesaj Gönderme
Ara
Çk. No:6,
08-13 14:37:58 | LBS
45%
aile üyeleri
Ana Sayfa
Ben


SAMSUNG
%68 14:47
MS
Takip Numarası
Uyarılar Bildirim Ayarları
Arama Ayarları
uzaktan kamera
Garip aramaları reddet
Saat Dilimi Seçimi
Saat Dili
LBS
Saati Sıfırla
Uzaktan kapatma
Ana Sayfa
Ben


SAMSUNG
%67 14:48
Fotoğraf
Düzenle
13-08-2022 14:48:03
Fotoğraf

“E ne güzel işte Mert, çocuğumuzu anlık olarak izleyebilir ve dinleyebiliriz” diye düşünüyor olabilirsiniz. Peki SeTracker2 uygulamasına giriş için kullandığınız e-posta adresinizi ve içinde özel karakter bile kullanarak güçlendiremediğiniz parolanızın bir an olsun art niyetli kişiler tarafından çalındığını veya tahmin edildiğini düşünelim. Art niyetli kişi, çocuğunuzun kolundaki saate uygulama üzerinden bağlanarak konumunu anlık olarak izleyebilir, fotoğrafını çekebilir, mesaj gönderebilir, gönderdiği mesajı silip geride iz bırakmayabilir, saatin belirttiği telefon numarasını aramasını sağlayarak ortam dinlemesi yaparak mahremiyetinizi, özel hayatınızın gizliliğini ihlal edebilir. Ayrıca art niyetli kişi tarafından gerçekleştirilen tüm bu işlemlerin iz kaydına (log) SeTracker2 uygulaması üzerinden ulaşma şansınızın olmadığının da altını çizeyim!

“Mert ben çok dikkatliyim, temkinliyim, kolay kolay dolandırıcıların ağına düşmem” de diyebilirsiniz. Aynı parolayı birden fazla web sitesine giriş esnasında kullanıyorsanız, o web sitelerinden biri çoktan hacklenmiş ve kullanıcı adınız/e-posta ve parolanız ele geçirilmiş olabilir. Çok Faktörlü Kimlik Doğrulaması (MFA) kullanmadığınız durumda (SeTracker2 uygulaması MFA desteklemiyor!) art niyetli kişilerin elde ettiği bu bilgilerle hesabınızın olduğu web sitelerine, mobil uygulamalara (SeTracker2 uygulaması gibi) rahatlıkla giriş yapılabileceğini unutmayın!

Çok faktörlü kimlik doğrulaması (MFA), kullanıcıların yalnızca bir paroladan daha fazla bilgi girmesini gerektiren, hesapta çok adımlı oturum açma sürecidir. Örneğin, kullanıcılardan parolanın yanı sıra e-posta adreslerine, cep telefonlarında gönderilen bir kodu (internet şubeye girişte olduğu gibi) girmeleri, mobil uygulamaya gönderilen bir isteği kabul etmeleri, gizli bir soruyu yanıtlamaları ya da parmak izlerini taratmaları istenebilir. İkinci bir doğrulama yöntemi, art niyetli kişilerin parolasını ele geçirildiği kullanıcıların hesaplarına yetkisiz erişmesini önlemeye yardımcı olmaktadır.

Bir diğer önemli konu ise ortam dinlemesi özelliğine sahip saatler kullanarak istemeden de olsa çocuğunuz üzerinden suç işliyor olabilirsiniz. Hukukçu olmasam da 5237 Sayılı Türk Ceza Kanunu’nun “Kişiler Arasındaki Konuşmaların dinlenmesi ve kayda alınması” başlıklı 133. maddesine dikkatinizi çekmek isterim:

(1) Kişiler arasındaki aleni olmayan konuşmaları, taraflardan herhangi birinin rızası olmaksızın bir aletle dinleyen veya bunları bir ses alma cihazı ile kaydeden kişi, iki yıldan beş yıla kadar hapis cezası ile

cezalandırılır.

(2) Katıldığı aleni olmayan bir söyleşiyi, diğer konuşanların rızası olmadan ses alma cihazı ile kayda alan kişi, altı aydan iki yıla kadar hapis veya adlî para cezası ile cezalandırılır.

(3) (Değişik: 2/7/2012-6352/80 md.) Kişiler arasındaki aleni olmayan konuşmaların kaydedilmesi suretiyle elde edilen verileri hukuka aykırı olarak ifşa eden kişi, iki yıldan beş yıla kadar hapis ve dörtbin güne kadar adlî para cezası ile cezalandırılır. İfşa edilen bu verilerin basın ve yayın yoluyla yayımlanması halinde de aynı cezaya hükmolunur.

Tahminimce başta Koş Mert Koş başlıklı blog yazım olmak üzere, güvenlik araştırmalarıma aşina olanlarınızın bu yazımda tersine mühendislikle, statik ve dinamik kod analizi ile SeTracker2 uygulamasını analiz edip tespit ettiğim zafiyetlerin nasıl kötüye kullanılabileceğini göstermemi veya saatte keşfettiğim donanımsal bir zafiyet ile saatin nasıl casus bir cihaza dönüştürebildiğini görmeyi umuyorlardı. Tüm bu anlattıklarımdan sonra bunca zahmete girmeden bu saatin, SeTracker2 uygulaması sayesinde art niyetli kişilere kötüye kullanım için davetiye çıkardığını, ebeveynler ve çocukları için büyük bir tehlike oluşturduklarını net olarak aktarabildiğimi düşünüyorum. :) Yine de uygulama ile ilgili teknik bilgi edinmek isteyenler var ise önceki yıllarda yapılmış olan çalışmalar için buraya ve de buraya göz atabilirler.

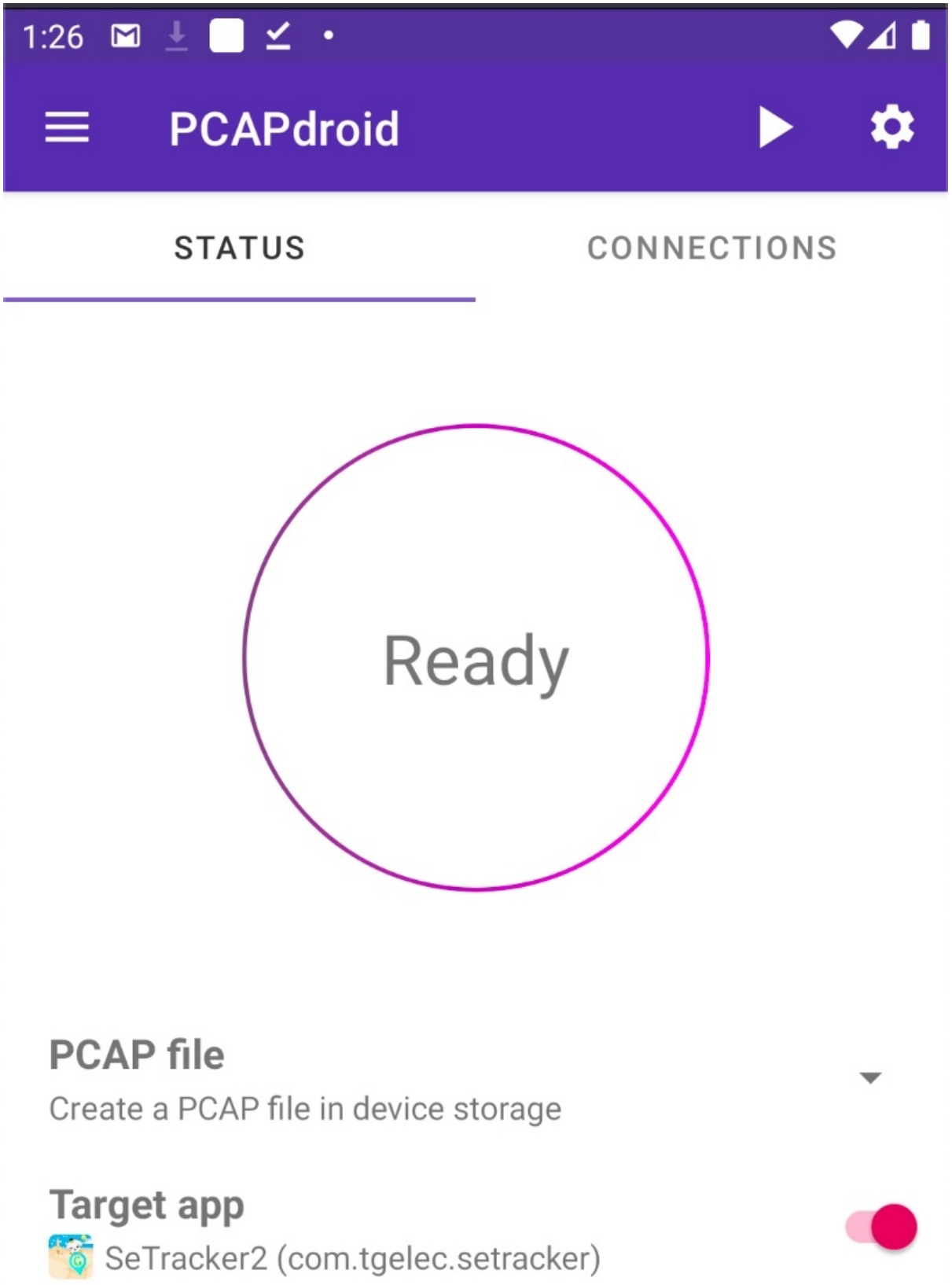
Umuyorum ki 2017 yılında Almanya'nın aldığı bu örnek karar gibi otoritelerimiz de benzer bir karar alarak, yasa dışı ortam dinlemesi yapma özelliğine sahip olan bu saat görünümlü potansiyel casus cihazların alışveriş sitelerinde satışını engelleyerek, ebeveynleri ve çocukları bu tür tehlikelerden korumak için önemli bir adım atarlar.

Bu bilgiler ışığında, ortam dinlemesi yapabilen akıllı çocuk saatleri kullanacaklara risklerini bilerek kullanmalarını tavsiye ettikten sonra siz sevgili okurlarımdan farkındalık yaratma adına bu yazıyı ebeveyn olan arkadaşlarınızla, dostlarınızla ve sevdiklerinizle paylaşmanızı önemle rica ederim.

Bir sonraki yazıda görüşmek dileğiyle herkese güvenli günler dilerim.

Not: Teknik okurlarım için de SeTracker2 uygulamasında SSL Pinning yönteminin kullanıldığını, HTTPS trafiğini analiz etmek için PCAPdroid isimli bir

Android uygulaması sayesinde basit bir şekilde trafiği kayıt altına aldığımı ve daha sonrasında da Wireshark aracı ile analiz edebildiğimi de paylaşayım.


1:26
PCAPdroid
STATUS
CONNECTIONS
Ready
PCAP file
Create a PCAP file in device storage
Target app
SeTracker2 (com.tgelec.setracker)



Collector port
1234

Traffic inspection

Block private DNS
Detect and possibly block private DNS to inspect DNS traffic. Disabling this can hinder traffic analysis

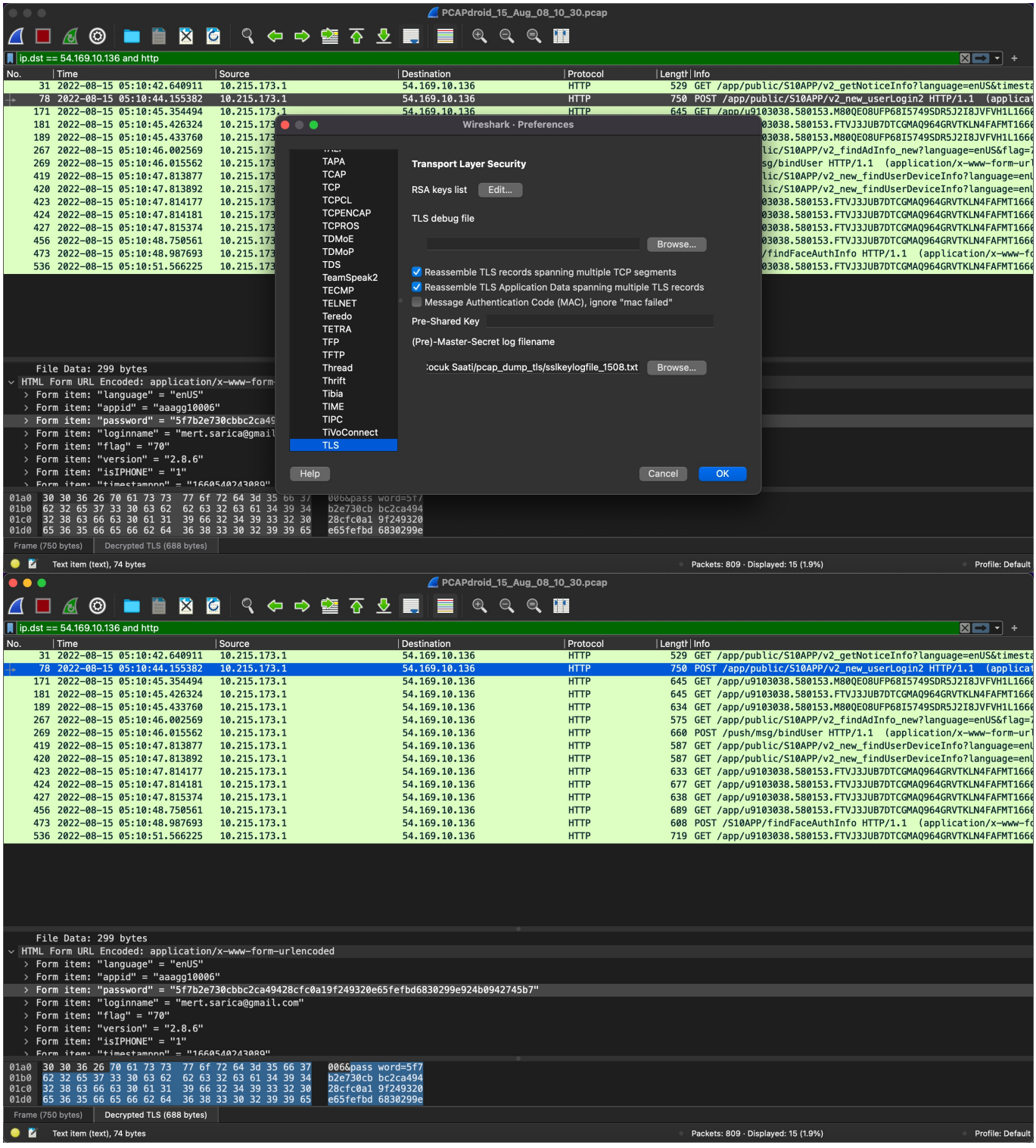
Geolocation
Show country and ASN info by performing offline lookups

TLS decryption
Decrypt the SSL/TLS traffic by performing mitm. This may now work with some apps, check out the user guide

Block QUIC
Block QUIC connections to possibly fall back to decryptable TLS. Some apps may stop working

Capture

Capture as root
Allows PCAPdroid to run with other VPN apps


PCAPdroid_15_Aug_08_10_30.pcap
ip.dst == 54.169.10.136 and http
No. Time Source Destination Protocol Length Info
31 2022-08-15 05:10:42.640911 10.215.173.1 54.169.10.136 HTTP 529 GET /app/public/S10APP/v2_getNoticeInfo?language=enUS&timesta
78 2022-08-15 05:10:44.155382 10.215.173.1 54.169.10.136 HTTP 750 POST /app/public/S10APP/v2_new_userLogin2 HTTP/1.1 (applicat
171 2022-08-15 05:10:45.354494 10.215.173.1 54.169.10.136 HTTP 645 GET /app/u9103038.580153.M80QE08UFP68I5749SDR5J2I8JVFVH1L1660
181 2022-08-15 05:10:45.426324 10.215.173.1 54.169.10.136 HTTP 645 GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1660
189 2022-08-15 05:10:45.433760 10.215.173.1 54.169.10.136 HTTP 634 GET /app/u9103038.580153.M80QE08UFP68I5749SDR5J2I8JVFVH1L1660
267 2022-08-15 05:10:46.002569 10.215.173.1 54.169.10.136 HTTP 575 GET /app/public/S10APP/v2_findAdInfo_new?language=enUS&flag=7
269 2022-08-15 05:10:46.015562 10.215.173.1 54.169.10.136 HTTP 660 POST /push/msg/bindUser HTTP/1.1 (application/x-www-form-url
419 2022-08-15 05:10:47.813877 10.215.173.1 54.169.10.136 HTTP 587 GET /app/public/S10APP/v2_new_findUserDeviceInfo?language=enU
420 2022-08-15 05:10:47.813892 10.215.173.1 54.169.10.136 HTTP 587 GET /app/public/S10APP/v2_new_findUserDeviceInfo?language=enU
423 2022-08-15 05:10:47.814177 10.215.173.1 54.169.10.136 HTTP 633 GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1660
424 2022-08-15 05:10:47.814181 10.215.173.1 54.169.10.136 HTTP 677 GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1660
427 2022-08-15 05:10:47.815374 10.215.173.1 54.169.10.136 HTTP 638 GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1660
456 2022-08-15 05:10:48.750561 10.215.173.1 54.169.10.136 HTTP 689 GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1660
473 2022-08-15 05:10:48.987693 10.215.173.1 54.169.10.136 HTTP 608 POST /S10APP/findFaceAuthInfo HTTP/1.1 (application/x-www-fo
536 2022-08-15 05:10:51.566225 10.215.173.1 54.169.10.136 HTTP 719 GET /app/u9103038.580153.FTVJ3JUB7DTCGMAQ964GRVTKLN4FAFMT1660
Wireshark · Preferences
TAPA
TCAP
TCP
TCPCL
TCPENCAP
TCPROS
TDMoE
TDMoP
TDS
TeamSpeak2
TECMP
TELNET
Teredo
TETRA
TFP
TFTP
Thread
Thrift
Tibia
TIME
TIPC
TiVoConnect
TLS
Transport Layer Security
RSA keys list
Edit...
TLS debug file
Browse...
Reassemble TLS records spanning multiple TCP segments
Reassemble TLS Application Data spanning multiple TLS records
Message Authentication Code (MAC), ignore "mac failed"
Pre-Shared Key
(Pre)-Master-Secret log filename
:ocuk Saati/pcap_dump_tls/sslkeylogfile_1508.txt
Browse...
Help
Cancel
OK
File Data: 299 bytes
HTML Form URL Encoded: application/x-www-form-urlencoded
Form item: "language" = "enUS"
Form item: "appid" = "aaagg10006"
Form item: "password" = "5f7b2e730cbbc2ca49428cfc0a19f249320e65fefbd6830299e924b0942745b7"
Form item: "loginname" = "mert.sarica@gmail.com"
Form item: "flag" = "70"
Form item: "version" = "2.8.6"
Form item: "isIPHONE" = "1"
01a0 30 30 36 26 70 61 73 73 77 6f 72 64 3d 35 66 37 006&pass word=5f7
01b0 62 32 65 37 33 30 63 62 62 63 32 63 61 34 39 34 b2e730cb bc2ca494
01c0 32 38 63 66 63 30 61 31 39 66 32 34 39 33 32 30 28cfc0a1 9f249320
01d0 65 36 35 66 65 66 62 64 36 38 33 30 32 39 39 65 e65fefbd 6830299e
Frame (750 bytes)
Decrypted TLS (688 bytes)
Text item (text), 74 bytes
Packets: 809 · Displayed: 15 (1.9%)
Profile: Default